FORTINET

High Performance Network Security

FortiWLM - Release Notes

Version 8.2.2

FortiWLM 8.2 introduces support for two new 802.11ac Wave2 access points, the FAP U421EV and FAP U423EV. The new Wave2 access points are dual radio, dual band 4x4 four stream 802.11ac Wave 2 access points designed to provide superior experience in data, voice, and video applications in enterprise class deployments.

Fortinet Universal Access Points

FAP-U421EV

FAP-U423EV

1. Radio profiles in WLM are not specific to AP models, so to use Wave-2 AP features like 4x4 MIMO and MU-MIMO, create separate radio profiles for FAPs and assign it to an AP group with only FAPs
2. FAP-U423EV and FAP-U421EV must be connected only to 802.3at PoE source. Connecting the APs to 802.3af source will not power the radios.

Additionally, this release also introduces features and enhancements as listed under the new features section.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Getting Started with Upgrade

This section describes procedures for upgrading your Services Appliance.

To upgrade legacy appliance SA2000 with serial number starting with **FWM2KM*****, contact customer support.

Pre-requisites for upgrade

- Upgrade service appliances (SA / FWLM) before you initiate controller (FortiWLC-SD) upgrade.

While upgrading a Services Appliance with over 100 controllers, the controllers return to *active* state sequentially, one at a time. It may take up to 10 minutes or more for all controllers to become active.

Supported Network Manager Upgrades

The following upgrade path is recommended:

- 6.1-2-28 and/or 6.1-3-6 > 8.0-7-0
- 7.0-5-0 > 8.0-7-0
- 8.0-7-0 > 8.1-2-0
- 8.0-SR1-1 >8.1-2-0
- 8.1-2-0 >8.2-2-0

Supported FortiWLC-SD Releases

Network Manager Version	Supports Controllers with these FortiWLC-SD Versions
8.2-1-0	• 7.0-9 • 8.0-5-0 • 8.0-SR1-2 • 8.1-2-0 • 8.2.3

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
FortiWLM/SAM - Access Points	• AP110 • AP122 • AP320 • AP332 • AP433 • OAP433 • AP822 • AP832 • AP1020 • AP1014 • OAP832 • PSM3X • FAP-U421EV (SAM not supported) • FAP-U423EV (SAM not supported)

Hardware / Software	Supported Versions/Models
SM	• AP332 • AP832 • PSM3x • AP822
Controllers	• FortiWLC-50D • FortiWLC-200D • FortiWLC-500D • MC1550 • MC1550-VE • MC3200 • MC3200-VE • MC4200 • MC4200-VE • MC5000 • MC6000
Service Appliance	• FortiWLM-100D • FortiWLM-1000D • SA250 • SA2000 • SA2000-VE • Hyper-V • KVM
Supported Browsers	• Internet Explorer 9 and later version *All the pages of EzRF will load under normal browser settings. Compatibility View Settings are not supported.* • Mozilla Firefox 32.0 • Google Chrome, version 34.0.1847.118 m

Upgrade Recommendations

VPN Controllers

With the introduction of SHA2 support in 8.1, any VPN controllers that are running SD version 8.0 or older and managed by WLM 8.1 or above will be disconnected from WLM after upgrade. To fix this issue, apply the following patches for SHA2 support. Patch images are available for download from support portal.

1. Upgrade your WLM to 8.1 using the steps mentioned in the Upgrade Procedure section.
2. Apply the following patches on the managed VPN controllers:
    a. In 7.0 or older controllers, apply the following patches using the **`patch controller <version>`** command
        - meru-7.0-9-1-patch-Bug0353345-generic-rpm.tar
        - meru-7.0-9-1-patch-Bug0363947-generic-rpm.tar
    b. In 8.0 controller, apply the following patches using the **`patch install <version>`** command or upload the patch from WebUI (**Maintenance** > **File Management** > **Patches**).
        - meru-8.0-6-0-patch-Bug0353345-generic-rpm.tar
        - meru-8.0-6-0-patch-Bug0363947-generic-rpm.tar

3. After applying the patch, disable and enable VPN Client stat in the WebUI (**Configuration** > **Security** > **VPN Client**).

Application Visibility Policies

Application visibility policies in controllers running SD 8.0 that is managed by WLM 8.1 or later will be disabled. To continue using those policies, upgrade SD to 8.1 or later.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

When upgrading from versions prior to FortiWLM 7.0, the DB is reset. It is therefore recommended that database backup should be taken before upgrade and restored after upgrade.

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
    a. Select **Service Assurance**.
    b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
    c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

    ```
    sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
    ```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

    ```
    sa# sh flash
    6.0-7-0
    8.2-1-0
    ```

7. Upgrade the service appliance:

    ```
    sa# upgrade nms-server <Version>
    ```

    This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes and at the end of the upgrade the services appliance restarts. The time taken to upgrade, depends on the size of the data available on the services appliance.

8. Type the following command to confirm, if the installed software version is 8.2.

    ```
    service appliance# sh nms
    ```

If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

Post Upgrade Tasks

The following are optional post upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration** > **Maintenance** page.
2. If required, upload the license.

Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

Downgrade

Downgrade is not supported. To go back to an older version of FortiWLM, you must do a fresh install of that version on your FortiWLM server.

New Features

Social Authentication Support in Captive Portal

The captive portal authentication process now supports Fortinet Presence as an external CP authentication server that allows users to authentication using social media accounts like Facebook or Gmail OAuth.

Supported APs: AP122, AP822, AP832, OAP832, FAP-U421, and FAP-U423.

Before proceeding, note the following:

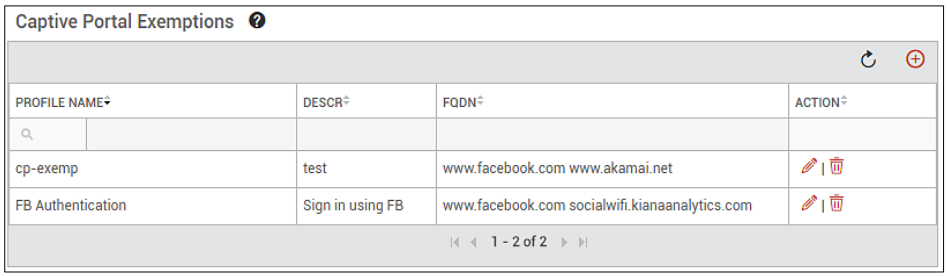
- Enable location service in the controller (See Configuring FortiPresence API section in the FortiWLC (SD) configuration guide for more details).
- Assign the AP in the data analytics store.
- Not supported in "Bridge mode".

To enable social authentication support, do the following:

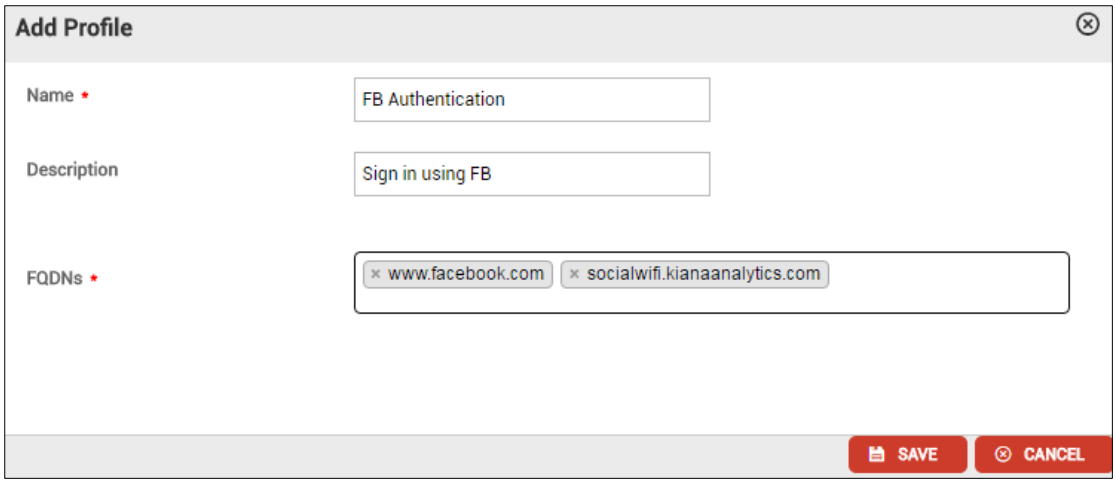
Create Captive Portal Exemptions Profile

To enable social login, create a profile with the list of exempted URLs and in the captive portal profile and select FortiPresence as the external authentication server.

1. Go to Configuration > Profiles > Captive Portal Exemptions.



2. Click the Add (**+**) button to create a profile with the list of URLs that will be allowed for social authentications. To add multiple URL to a profile, enter a space after each URL entry. You can add up to 32 URLs.

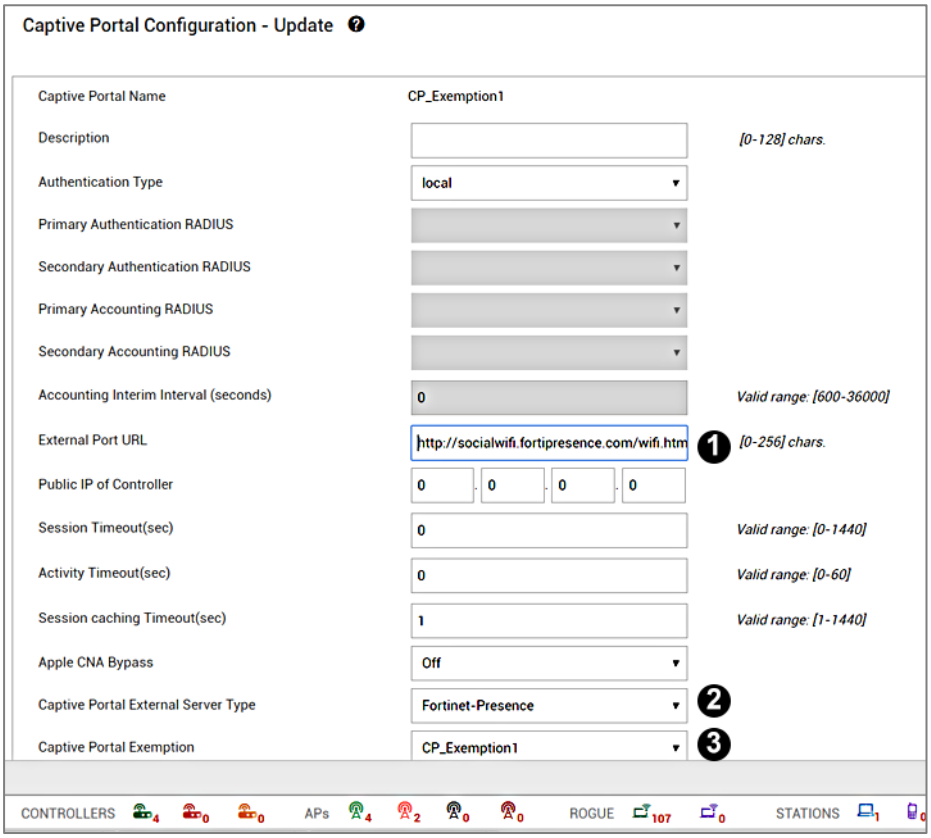


For each profile, ensure that you add **socialwifi.fortipresence.com** (inclusive of the 32 URLs) as part of the FQDN list. This is mandatory for clients to access Social Wi-Fi login page.

Configure Captive Portal Profile to use Fortinet Presence

1. Go to Configuration > Profiles > Captive Portal
2. Create a captive portal profile with ***local*** or ***radius*** as authentication type.
    a. If Authentication type is ***Local***, then create a guest user with the following credentials (*in the controller*):
        - username: `gooduser`
        - password:good.
    b. If Authentication type is ***RADIUS***, then in that RADIUS server, create a user with the following credentials:
        - username: `gooduser`
        - password:good.

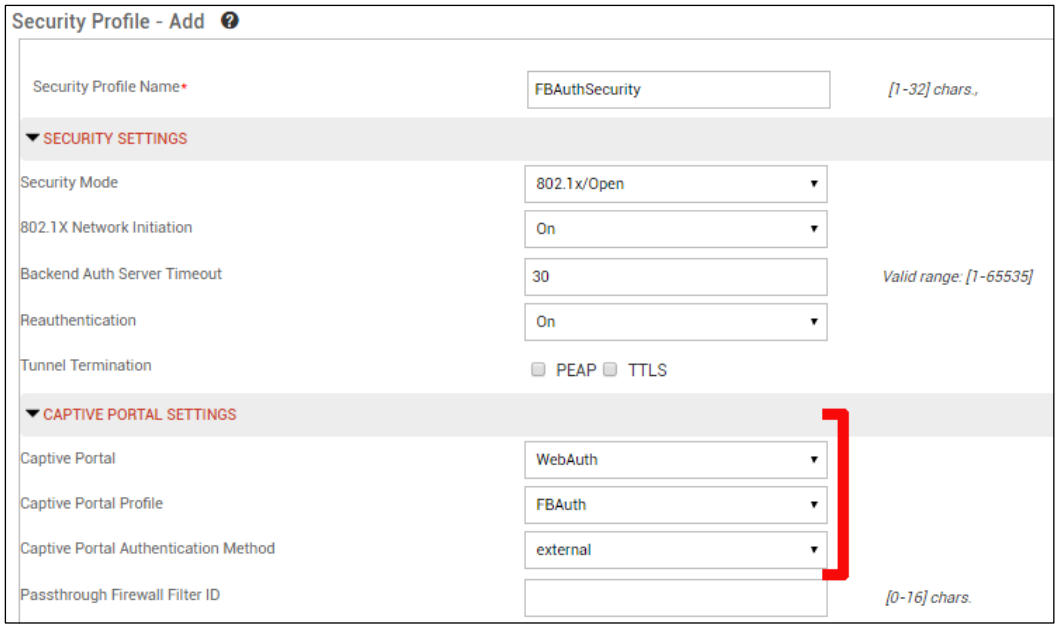
2. Make the following changes to External Portal Settings:



1. Enter the **http://socialwifi.fortipresence.com/wifi.html?login** URL (**1**) in the external portal URL.
2. Select Fortinet-Presence as the external server (**2**).
3. Select the profile (**3**) created with the exempted URLs.

Enable this captive portal profile in security and ESS profiles

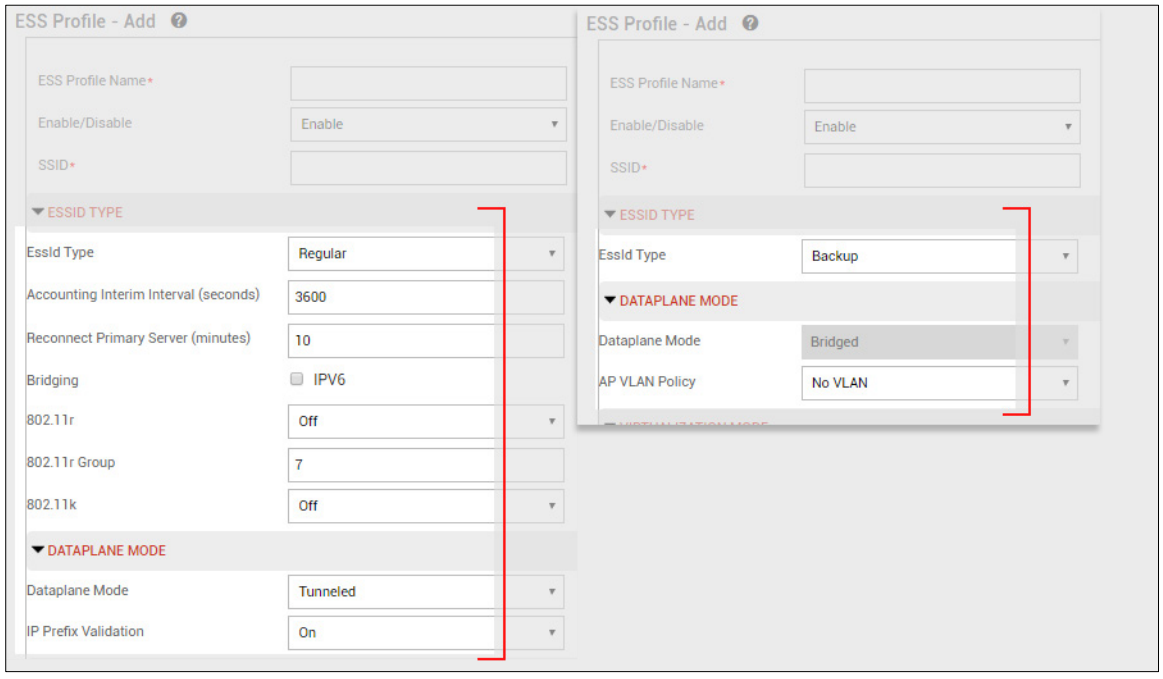
Enable the captive portal profile in the security profile and map the security profile in the ESS Profile. In the security profile, make the following changes to the CAPTIVE PORTAL SETTINGS section:



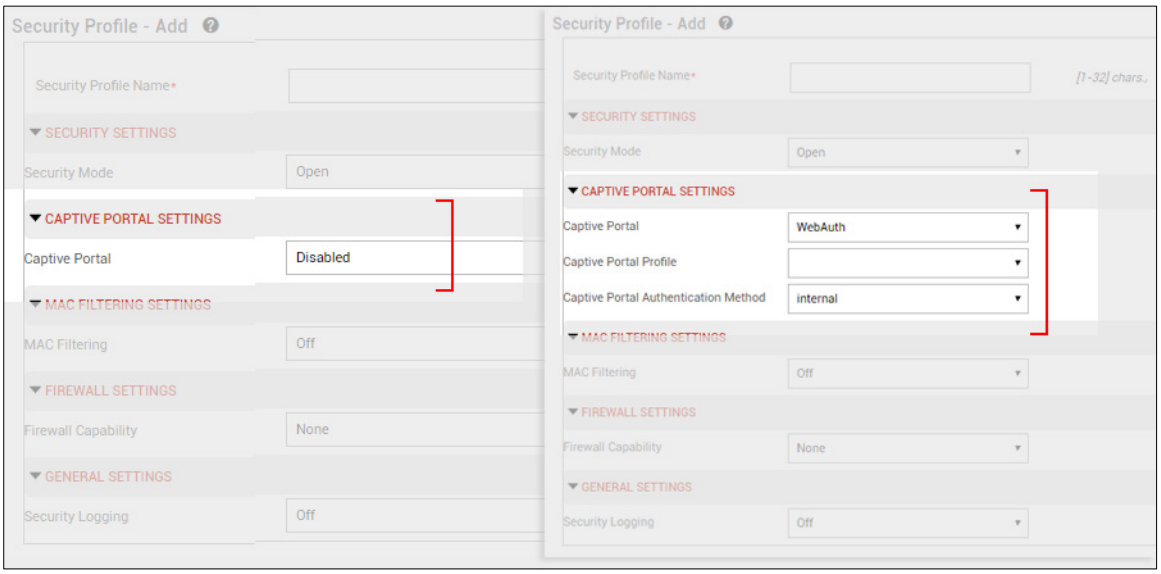
Logical Grouping of ESS and Security Config Options

Starting with the 8.2 release, ESS and Security profile config options in the WebUI are grouped logically to help in easy configuration. Within the logical groups' only dependent configuration options of a parameter are visible. For example, in an ESS profile selecting the Essid Type as Backup, shows parameters that are applicable only for a backup ESS profile.

ESS Profile

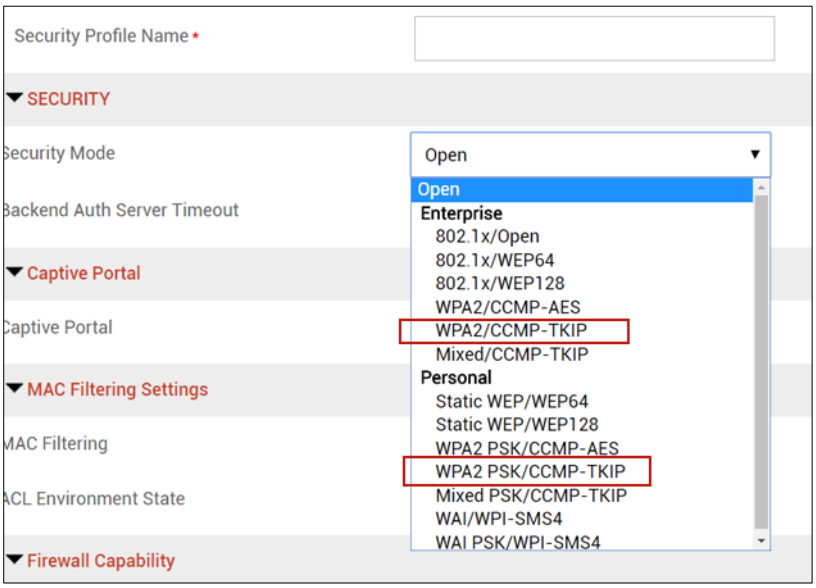


Security Profile



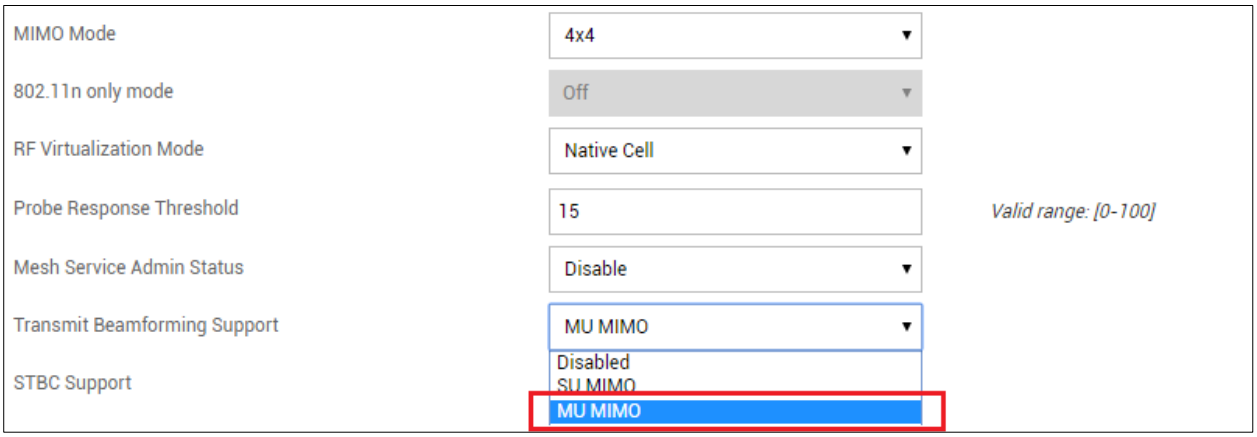
Support for WPA2-TKIP encryption

You can now create a security profile with WPA2-TKIP encryption. This option is available in the security mode dropdown list in the security profile configuration page (Configuration > Security > Profile (Add and Edit pages)):



MU-MIMO Configuration

A new configuration parameter MU-MIMO is added to the radio configuration. If your network has MU-MIMO capable clients (802.11ac Wave 2), then we recommend enabling this parameter. By default, this option is enabled.



Licensing Changes

As part of a fresh installation on FortiWLM-100D and FortiWLM-1000D, permanent licenses for 50 NM, 2 SAM & 2 SM are enabled by default.

For other hardware installations, you will be required to enable 30 day trial license or apply a license file.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service